

## OVPRS Research Privacy-Data Broker Best Practices: De-Identified Images

### Introduction

Research Privacy/Data Broker Services provides guidelines for de-identifying provisioned photographs to University/UHealth employees. These guidelines are subject to updates based on new de-identification features for images ([HP 44.0 - Creation of Fully De-Identified Information, PolicyStatID:12390957](#); [HP 43.0 - Receipt of Facially De-Identified Information, PolicyStatID:8863595](#)).

### Expectations of Researcher

When researchers are provided with images, there are several key expectations to ensure that the use of images in research is conducted ethically and responsibly, protecting the rights and privacy of participants while enabling valuable scientific inquiry.

Expectations	
Data Privacy and Confidentiality	<ul style="list-style-type: none"> <li>Researchers must ensure that the privacy of participants is protected. This includes anonymizing images where necessary and implementing robust data security measures to prevent unauthorized access.</li> </ul>
Ethical Use	<ul style="list-style-type: none"> <li>Researchers should use the images strictly for the purposes outlined in their research proposal.</li> </ul>
Transparency	<ul style="list-style-type: none"> <li>Researchers need to be transparent about how the images will be used, stored, and shared. This includes providing clear information to participants (if applicable) about the scope and nature of the research</li> </ul>
Compliance with Regulations	<ul style="list-style-type: none"> <li>Researchers must comply with all relevant legal and institutional regulations regarding the use of images in research.</li> </ul>
Documentation and Reporting	<ul style="list-style-type: none"> <li>Proper documentation of how images are used in the research is essential. This includes maintaining records of consent (if applicable), data handling procedures, and any analysis conducted using the images</li> </ul>
Respect for Participants	<ul style="list-style-type: none"> <li>Researchers should respect the dignity and rights of participants whose images are used. This includes avoiding any use of images that could cause harm or distress to the participants</li> </ul>

### Agreements/Authorizations for Research

Items	Details	Recommended Forms
Research Photo Authorization	<ul style="list-style-type: none"> <li>If identifiable photos are being obtained for the purposes of a research study, then language to this effect should be explicitly included in the Informed Consent Form (ICF)/authorization documents.</li> <li>Human Subjects Research Office (HSRO) - Research Authorization/Release for Photography or Audio/Video Recordings in a Research Study.</li> </ul>	<ul style="list-style-type: none"> <li>Research ICF/Authorization language or HSRO Authorization for Photography or Audio/Video Recordings</li> </ul>

Waiver of Informed Consent	<ul style="list-style-type: none"> <li>An IRB waiver of informed consent for sharing images with researchers allows the use of images in research without obtaining explicit consent from participants under certain conditions.</li> </ul>	<ul style="list-style-type: none"> <li>HRP-410-CHECKLIST: Waiver or Alteration of Consent Process</li> </ul>
Current Partnership Related to Vendor	<ul style="list-style-type: none"> <li>If identifiable images are being obtained to be shared with external vendors for AI research, the UHealth HIPAA Contracts team is available to conduct/execute an assessment for a Business Associate Agreement (BAA).</li> </ul>	<ul style="list-style-type: none"> <li>Business Associate Agreement (BAA)</li> </ul>
Other Applicable Agreements	<ul style="list-style-type: none"> <li>If photos are being shared with an external entity, then depending on specifics of project/collaboration, a suitable agreement needs to be executed.</li> <li>UHealth Medical Communications, Supply Chain/Business Services <u>and/or General Counsel</u> can be reached for guidance and/or approval.</li> </ul>	<ul style="list-style-type: none"> <li>Use of Name Agreement, Collaboration Agreement etc.</li> </ul>
Future Partnership Related to Vendor	<ul style="list-style-type: none"> <li>The UHealth HIPAA Contracts team is available to conduct an assessment for a Business Associate Agreement (BAA) when there is a need to share images containing personal identifiers with a vendor for de-identification purposes.</li> <li>BAA Determination Requests: send to <a href="mailto:HIPAAContracts@miami.edu">HIPAAContracts@miami.edu</a>.</li> <li>If there is no need for a BAA, then a different agreement type may be necessary, depending on the specifics of the relationship.</li> </ul>	<ul style="list-style-type: none"> <li>Business Associate Agreement (BAA)</li> </ul>

#### Agreements/Authorizations for Non-Research

Items	Details	Recommended Forms
Patient Photo Authorization	<ul style="list-style-type: none"> <li>Recommended to obtain a patient photo authorization form for any non-direct related healthcare reason.</li> <li>Examples would include marketing and publication.</li> </ul>	<ul style="list-style-type: none"> <li>Health Information Management (HIM) Authorization/Release for Photography or Audio/Video Recording form.</li> </ul>
Other Applicable Agreement	<ul style="list-style-type: none"> <li>If photos are being shared with an external entity, then depending on specifics of project/collaboration, a suitable agreement needs to be executed.</li> </ul>	<ul style="list-style-type: none"> <li>Use of Name Agreement</li> </ul>

	<ul style="list-style-type: none"> <li>UHealth Medical Communications, Supply Chain/Business Services and/or <u>General Counsel</u> can be reached for guidance and/or approval.</li> </ul>	
Future Partnership related to Vendor	<ul style="list-style-type: none"> <li>The UHealth HIPAA Contracts team is available to conduct an assessment for a Business Associate Agreement (BAA) when there is a need to share images containing personal identifiers with a vendor for de-identification purposes.</li> <li>BAA Determination Requests: send to HIPAAContracts@miami.edu.</li> </ul>	<ul style="list-style-type: none"> <li>Business Associate Agreement (BAA)</li> </ul>

### What is De-Identification?

De-identification is the process of removing or obscuring personal identifiers from data sets, such as photographs, to protect the privacy of individuals. This reduces the risk that the data can be traced back to the individual, thereby complying with privacy regulations like HIPAA. In the context of images, de-identification involves removing or altering features that could reveal the identity of the person, such as faces, tattoos, distinctive marks, and related metadata.

### De-Identification Process

Step	Details
Project Team De-identification Process	<ul style="list-style-type: none"> <li>Document the de-identification process, including how images will be de-identified, where the de-identified images will be stored, who will validate the de-identified images, and process for transferring the de-identified images to the vendor, if required.</li> <li>De-identifying photos involves removing or altering information that can be used to identify individuals. This process is crucial, especially when handling sensitive information like Protected Health Information (PHI) under regulations such as the Health Insurance Portability and Accountability Act (HIPAA)</li> </ul>
Patient Consent	<ul style="list-style-type: none"> <li>If possible, obtain consent from individuals in the photo for the specific use of their de-identified images. This is in the interest of transparency. There is always a risk of re-identification, especially for facial images.</li> </ul>
Data Sharing	<ul style="list-style-type: none"> <li>Photos to be shared internally with authorized members involved in the de-identification process.</li> <li>UHealth IT offers these options to provision the images: <ul style="list-style-type: none"> <li>UM Box</li> <li>UHealth IT File share</li> <li>Potentially UHealth-managed Cloud Storage account.</li> </ul> </li> <li>For large volumes of images/photos (1TB-5TB), complete the <a href="#">"UHealth IT Create a new UHealth IT File-Share or Request a space increase of an existing UHealth IT File-Share"</a> to be able to provision the images</li> </ul>

Safe Harbor Guidance	<ul style="list-style-type: none"> <li>• <a href="#">Follow the safe harbor guidance which includes removing all 18 types of identifiers listed by HIPAA, such as names, geographic subdivisions smaller than a state, all elements of dates (except year), and other unique identifying numbers or codes</a><sup>1</sup>.</li> <li>• This data can sometimes be “embedded” into a photo or can be in the properties of the file.</li> </ul>
Important Note	<ul style="list-style-type: none"> <li>• Remember, while de-identification attempts to reduce the risk of identifying individuals, it does not eliminate it entirely.</li> <li>• Review the Agreements/Authorizations for Research and Agreements/Authorizations for Non-Research sections.</li> <li>• Review the <a href="#">HP 44.0 - Creation of Fully De-Identified Information, PolicyStatID:12390957</a>, and <a href="#">HP 43.0 - Receipt of Facially De-Identified Information, PolicyStatID:8863595</a></li> <li>• <a href="#">Always consider the context in which the de-identified photos will be used and the potential for re-identification in that context.</a></li> <li>• Consult UHealth IT for data sharing options or Research Privacy/Data Broker for de-identification best practices as needed.</li> <li>• <a href="#">For detailed guidance, you can refer to the official documents provided by HHS on de-identification methods</a></li> </ul>

### De-Identification Process Phases

Phase	Details
Preparation Phase	<ul style="list-style-type: none"> <li>• Assessment of Images: The study team assesses the images to identify any potential identifiers that need to be removed.</li> <li>• Expert Determination: Engage the data custodian/data steward to analyze the risk of re-identification. The data custodian/data steward should have knowledge of the methods used to mask or remove identifiers and assess the likelihood that someone could be recognized.</li> <li>• Consultation: If necessary, consult with IT for initial de-identification guidance on complex cases. Another possible source of expertise may be UHealth Imaging Groups/Admins.</li> </ul>
De-Identification Phase	<ul style="list-style-type: none"> <li>• Removal of Identifiers: Using image editing software, remove or obscure all direct and indirect identifiers such as faces, tattoos, scars, birthmarks, jewelry, clothing, photos of distinctive injuries, or other identifying features that could reveal the individual’s identity.</li> <li>• Sensitive Content: Remove sensitive content from PDFs in Adobe Acrobat</li> <li>• Tagging: Images without Patient Number and names should be tagged with an alternate identifier. This is especially important if there is additional information e.g., demographics, Social Determinants of Health (SDOH), that need to accompany the corresponding images, as part of the requirements for the specific project.</li> <li>• Pixelation or Blurring: Apply pixelation or blurring to faces or other identifiable features in the image. The level of alteration should be sufficient to prevent recognition.</li> <li>• Cropping: Crop out any parts of the image that contain identifiable information, such as name tags, house numbers, or distinctive landmarks.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Overlays:</b> Use solid color overlays to cover faces or other personal identifiers.</li> <li>• <b>Metadata Removal:</b> Ensure that all metadata, which can include location information and timestamps, as well as direct identifiers, is stripped from the image file.</li> <li>• <b>Quality Check:</b> After editing, perform a quality check to ensure all identifiers have been adequately de-identified. Also, ensure that the above steps taken to remove/obscure identifiers are not reversible using either the original software or alternate software applications.</li> </ul>
Validation Phase	<ul style="list-style-type: none"> <li>• <b>Internal Review:</b> Designated team members review the de-identified images to validate the removal of identifiers.</li> <li>• <b>Documentation:</b> Document the review process, noting the date, person conducting the review, and any issues identified.</li> </ul>
Storage Phase	<ul style="list-style-type: none"> <li>• <b>Secure Storage:</b> Store images in approved UM storage devices, access-controlled environment.</li> <li>• <b>Backup:</b> Ensure backups are created and stored separately to prevent data loss.</li> </ul>
Transfer Phase (if applicable)	<ul style="list-style-type: none"> <li>• <b>Secure Transfer:</b> If images are to be shared with a vendor, use secure transfer methods such as encrypted email or secure file transfer protocols. Consult UHealth IT Cybersecurity for suitable methods, depending on file sizes, frequency, and volume.</li> <li>• <b>UHealth Governance, Risk, and Compliance-HIPAA Request Form</b> is required for data transmission involving PHI fields.</li> <li>• <b>Record Keeping:</b> Maintain records of all transfers, including the recipient, date, and transfer method.</li> </ul>
Receipt Phase (if applicable)	<ul style="list-style-type: none"> <li>• <b>Secure Transfer:</b> If images are to be received from a vendor, use secure transfer methods such as encrypted email or secure file transfer protocols. Consult UHealth IT Cybersecurity for suitable methods, depending on file sizes, frequency, and volume.</li> <li>• <b>UHealth Governance, Risk, and Compliance-HIPAA Request Form</b> is required for data transmission involving PHI fields.</li> <li>• <b>Record Keeping:</b> Maintain records of all receipts, including the recipient, date, and transfer method.</li> <li>• <b>Review referenced policy:</b> <a href="#">HP 43.0 - Receipt of Facially De-Identified Information, PolicyStatID:8863595</a>)</li> </ul>
Ongoing Monitoring	<ul style="list-style-type: none"> <li>• Regularly review de-identification standards and practices, as technology and re-identification techniques evolve over time.</li> <li>• <b>Updates to Process:</b> Stay informed about new de-identification techniques and update the process, as necessary.</li> </ul>
Training	<ul style="list-style-type: none"> <li>• <b>Staff Training:</b> Provide regular staff training involved in the de-identification process to ensure they are aware of the latest guidelines and techniques.</li> <li>• <b>Refresher Courses:</b> Offer refresher courses to keep the knowledge current and address any new challenges that may arise.</li> </ul>
Compliance	<ul style="list-style-type: none"> <li>• <b>Regulatory Compliance:</b> Ensure that the de-identification process complies with all relevant regulations and standards, such as HIPAA and applicable UM policies.</li> </ul>

	<ul style="list-style-type: none"> <li>• Documentation for Compliance: Keep detailed records of the de-identification process to demonstrate compliance during audits or inspections.</li> <li>• Consider if there is a need to retain identifiable images.</li> </ul>
--	--

### De-Identification Common Challenges

Challenge	Details
Complex Identifiers	<ul style="list-style-type: none"> <li>• Identifiers in images can be more complex than just text data. Things like scars, tattoos, or even the background of a photo can reveal personal information.</li> </ul>
Quality of De-identification	<ul style="list-style-type: none"> <li>• Ensuring that the de-identification is thorough while maintaining the usefulness of the image for research or clinical purposes can be difficult.</li> </ul>
Re-identification Risks	<ul style="list-style-type: none"> <li>• There is always a risk that de-identified data can be re-identified, especially with the advancement of technology and data linkage methods.</li> </ul>
Balancing Privacy and Utility	<ul style="list-style-type: none"> <li>• Striking the right balance between protecting patient privacy and retaining the scientific value of the images is a delicate task.</li> </ul>
Legal and Ethical Considerations	<ul style="list-style-type: none"> <li>• Navigating the legal requirements for de-identification and ensuring ethical use of the images can be complex.</li> </ul>
Consistency	<ul style="list-style-type: none"> <li>• Maintaining consistency in de-identification practices across different datasets and time points to ensure comparability can be challenging.</li> </ul>
Time and Resources	<ul style="list-style-type: none"> <li>• De-identification can be time-consuming and resource-intensive, especially for large datasets.</li> </ul>
Training and Awareness	<ul style="list-style-type: none"> <li>• Ensuring that all personnel involved are adequately trained and aware of the importance of de-identification.</li> </ul>
Evolving Standards	<ul style="list-style-type: none"> <li>• Keeping up with evolving standards and best practices in de-identification as technology and regulations change.</li> </ul>

### Precautions using Cloud-based applications for De-Identification

Step	Details
Study Team	<ul style="list-style-type: none"> <li>• Cloud-based applications for de-identification of images can be tempting to use, but it is important to take certain precautions to ensure data security and privacy</li> </ul>
Data Security & Privacy	<ul style="list-style-type: none"> <li>• Storing and processing images in the cloud can expose them to potential data breaches. Always use UM-approved and managed resources.</li> <li>• Ensuring that sensitive images are protected from unauthorized access is crucial.</li> <li>• Frequently the application may require uploading of the identifiable images before processing to “de-identify.” It may not be entirely clear if the identifiable image remains “stored” in the application, even if not visible.</li> <li>• Uploading images to a server or storage location that is not part of UM/UHealth is considered a disclosure of information. As a result, it is necessary to establish a Business Associate Agreement (BAA) or a Data</li> </ul>

	<p>Use Agreement (DUA) with the owner of the destination server or storage location.</p> <ul style="list-style-type: none"> <li>Only use applications reviewed and vetted by UM/UHealth IT or otherwise approved via an agreement or by a University/UHealth Compliance area.</li> </ul>
Compliance and Legal Concerns	<ul style="list-style-type: none"> <li>Ensuring compliance with data protection regulations like GDPR or HIPAA can be challenging. Non-compliance can result in legal penalties and loss of trust</li> </ul>
Misconfiguration Risks	<ul style="list-style-type: none"> <li>Incorrectly configured cloud services can leave data vulnerable. Misconfigurations are a common cause of data leaks and can occur due to human error</li> </ul>
Data Minimization	<ul style="list-style-type: none"> <li>Only collect and retain the minimum amount of data necessary for your purposes. This reduces the risk of exposure.</li> </ul>
Storage	<ul style="list-style-type: none"> <li>Images can be saved in the application directory on the UM provided local computer temporarily or in a UM approved cloud-based application storage</li> </ul>
Application Samples	<ul style="list-style-type: none"> <li>Adobe Creative Cloud Suite (Photoshop, Adobe Express, Acrobat), Snagit, Microsoft Snipping Tool, Canva, Pixlr PicWish, Fotor</li> </ul>
File Type Samples	<ul style="list-style-type: none"> <li>JPEG (Joint Photographic Experts Group), PNG (Portable Network Graphics), TIFF (Tagged Image File Format), WebP by Google, AVIF (AV1 Image File Format, HEIF (High-Efficiency Image Format): Used by Apple</li> </ul>

### Departments, Forms, and Contacts

Form	Department Owner	Contact Information
Authorization/Release for Photography or Audio/Video Recording form	UHealth Health Information Management (HIM)	Email: <a href="mailto:privacy@med.miami.edu">privacy@med.miami.edu</a> or <a href="mailto:uchartecopy@med.miami.edu">uchartecopy@med.miami.edu</a>
Use of Name Agreement	UHealth Medical Communications, Supply Chain/Business Services, and/or General Counsel	Email: <a href="mailto:medcommunications@miami.edu">medcommunications@miami.edu</a>
Research Authorization/Release for Photography or Audio/Video Recording form	OVPRS Human Subjects Research Office (HSRO)	Email: <a href="mailto:hsro@miami.edu">hsro@miami.edu</a>  Website: <a href="https://hsro.uresearch.miami.edu/index.html">https://hsro.uresearch.miami.edu/index.html</a>
HRP-410-CHECKLIST: Waiver or Alteration of Consent Process	OVPRS Human Subjects Research Office (HSRO)	Website: <a href="https://hsro.uresearch.miami.edu/resources-and-guidance/informed-consent/waivers/index.html">https://hsro.uresearch.miami.edu/resources-and-guidance/informed-consent/waivers/index.html</a>
UHealth IT Cybersecurity HIPAA Transmitting/Receiving App	UHIT Governance, Risk, and Compliance	Email: <a href="mailto:UHIT-GRC@med.miami.edu">UHIT-GRC@med.miami.edu</a>
Business Associate Agreement (BAA)	UHealth HIPAA Contracts team	Email: <a href="mailto:HIPAAContracts@miami.edu">HIPAAContracts@miami.edu</a> .

Data Broker Service Data Handling Guidelines and Safe Harbor Guidance	OVPRS Research Privacy-Data Broker Services	<p>Email: <a href="mailto:databroker@miami.edu">databroker@miami.edu</a></p> <p>Website:  <a href="https://www.research.miami.edu/about/admin-areas/privacy/data-brokers/data-handling-guidelines/index.html">https://www.research.miami.edu/about/admin-areas/privacy/data-brokers/data-handling-guidelines/index.html</a>  +  <a href="https://www.research.miami.edu/about/admin-areas/privacy/data-brokers/data-minimization/index.html">https://www.research.miami.edu/about/admin-areas/privacy/data-brokers/data-minimization/index.html</a></p>
HP 44.0 - Creation of Fully De-Identified Information, PolicyStatID:12390957	UHealth Privacy Office	<p>Email: <a href="mailto:privacy@med.miami.edu">privacy@med.miami.edu</a></p> <p>Website:  <a href="https://umhs-ummg.policystat.com/policy/12390957/latest/">https://umhs-ummg.policystat.com/policy/12390957/latest/</a></p>
HP 43.0 - Receipt of Facially De-Identified Information, PolicyStatID:8863595)	UHealth Privacy Office	<p>Email: <a href="mailto:privacy@med.miami.edu">privacy@med.miami.edu</a></p> <p>Website:  <a href="https://umhs-ummg.policystat.com/policy/8863595/latest/">https://umhs-ummg.policystat.com/policy/8863595/latest/</a></p>